Data Security Model for Internet-Based Environment With Quantum Computing

Akomolafe, O.P., Ikudaisi .D.O, & Akanji W.A
Department of Computer Science
University of Ibadan
Ibadan, Oyo State, Nigeria
E-mail: davetoba01@gmail.com

ABSTRACT

Security and privacy is a critical challenge in internet environments. The most common and recent security measure used in protecting data on transit is the use of TLS/SSL cryptography protocol which has significant drawbacks. A potential drawback of TLS/SSL cryptography protocol is that it is vulnerable to eavesdropping attack due to the fact that during TLS/SSL cryptography protocol handshaking process the negotiation process between the client and the server is done via unencrypted communication channel which shows the weakness in the use of TLS/SSL cryptography protocol as the attacker can intercept the communication channel posing as potential client or server. To overcome the drawback in TLS/SSL cryptography protocol this paper propose a QKDSSL cryptography system that is resistant to eavesdropping attack for data in transit on a network.

Keywords: Quantum Key Distribution, Vulnerable, Protocol, Encrypted, Multi-Cloud, Transit

1. INTRODUCTION

Internet based computing is one of the fastest growing technology emerging in the field of Information Technology, it allows sharing of sensitive information over the internet using any internet accessible devices. In today's technical environment many latest technologies are changing the face of the mankind. But due to these emerging technologies the rate of internet crime are increasing day by day due to the fact that sensitive information are usually sent over the internet. Today more than 60% of total commercial transactions are done online, so this field required a high quality of security for transparent and best transactions over the internet. The information collected and communicated across the internet may contain sensitive information. It is essential that security and privacy of user information both at rest and on transit should be taken more into consideration. Thus, the trend of the near future appears to be that an increasing fraction of the internet communication between client and the server is protected by end-to-end encryption (TLS/SSL cryptography protocol)

1.1 Possible Internet Attacks And Their Counter Measure

Internet environment is not much secure by nature. Internet security is not exactly tangible hence there a false sense of security and anxiety about how user data is actually secured and controlled. There are concerns related to the integrity and confidentiality of data. As shown in figure 1.0, Internet attacks are classified into different types such as eves dropping, Man-in-the-Middle attack, replay attack, brute force and dictionary attack, insider attack, key logger attack, phishing attack, Shoulder surfing attack and session hijacking attack [2].

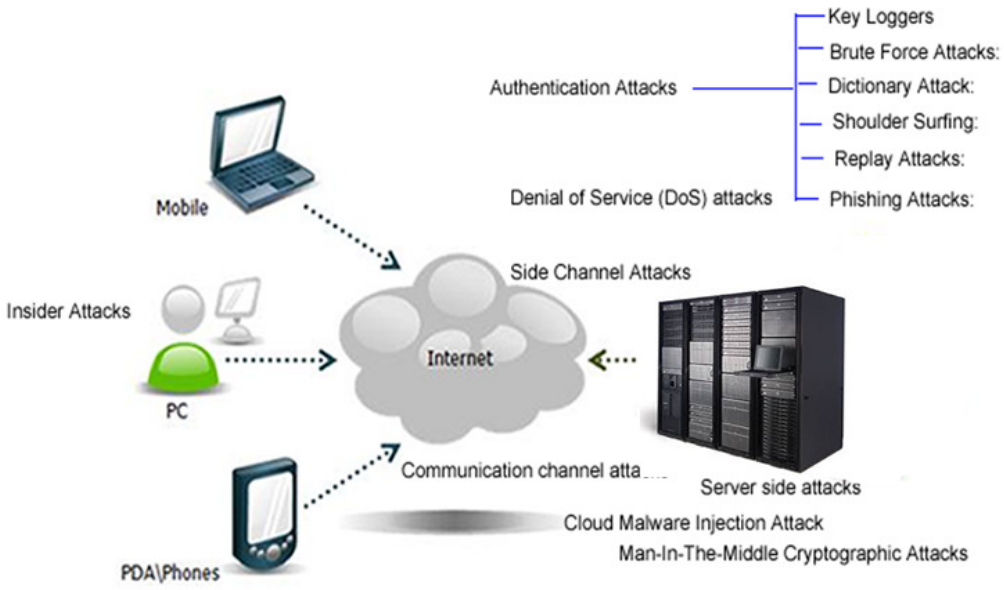

Figure 1.0: Various attack in Internet environment.

1.2 Problem Statement

One way of mitigating a potential attack during a user's session to secure data communication in recent research is the use of TLS/SSL protocol to encrypt data communication channel between the user and the server. During SSL/TLS handshaking process messages are not protected and that is why each endpoint sends a "change cipher spec" before finishing the handshake. With these view it was observed that SSL protocol can be vulnerable to eavesdropping attack, where an attacker can delete the "change cipher spec" message so that the server and client will never upgrade their current cipher suite. As a solution to this problem, this research propose a better framework where Quantum Computing idea will be integrated with SSL/TLS cryptography protocol to solve the Cipher Suite Rollback attack in cloud environment by eavesdropper.

2. PROPOSED SYSTEM

The system uses QKD (Quantum Key Distribution) for exchange of key (in form of photons) in a particular polarization (Rectilinear or Diagonal) pattern between the user and the server instead of negotiating on unencrypted channel during TLS/SSL cryptography protocol handshaking process. This is done to prevent Man-In-The-Middle attack. For attacker to be able to succeed, the attacker must get the right polarization pattern used in exchange of key (in photon form) between the client and the server.

2.1 How Key Is Exchange Between Client And Server Internet-Based Environment Using Quantum Computing

Table 2.0, shows how client and the server exchange key in form of photon which are 0 or 1 using quantum computing. In negotiating key between the client and the server, the two sides must decide on the same polarization pattern for the photon [4].

Table 1: How Information Are Represented Using Photon

Spin	Horizontal Spin (-)	Vertical Spin (|)	Left Diagonal Spin (\)	Right Diagonal Spin(/)
Value	0	1	0	1

3. ARCHITECTURAL DESIGN

Architectural design is the process for identifying the sub-system that make up a system and the framework for sub-system control and communication. In other words, architectural design partitions the functional requirement of a system into a manageable set of interacting elements. Actually, before any coding and implementation the attributes of qualification such as usability and security can be appraised and approved in this stage as shown in figure 3.0.

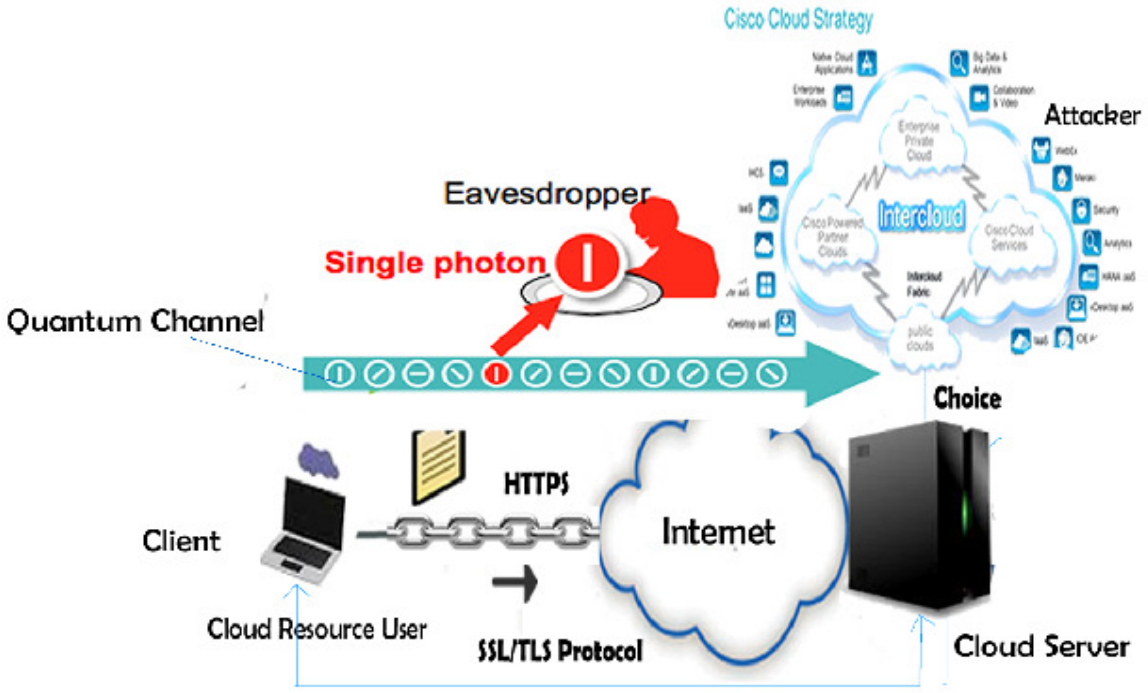

Figure 3.0: Architectural design of the system

3.2 Integration Of Quantum Computing Into TLS/SSL Handshaking Process

The client and the server start the Quantum cryptography protocol to derive a key K which the security is guaranteed by the laws of quantum physics.

$K = \{0,1\}^N$

As mentioned before, the TLS/SSL protocol is vulnerable to "eavesdropping" attack, so to check if the mutual authentication is established correctly, the user and the server must calculate the TLS/SSL finished message using the shared secret S and the key generated by the processes of Quantum Key Distribution.

pre _ master _ secret = K + S
master _ secret = PRF (*pre _ master _ secret , "master secret ", ClientHello.random)*

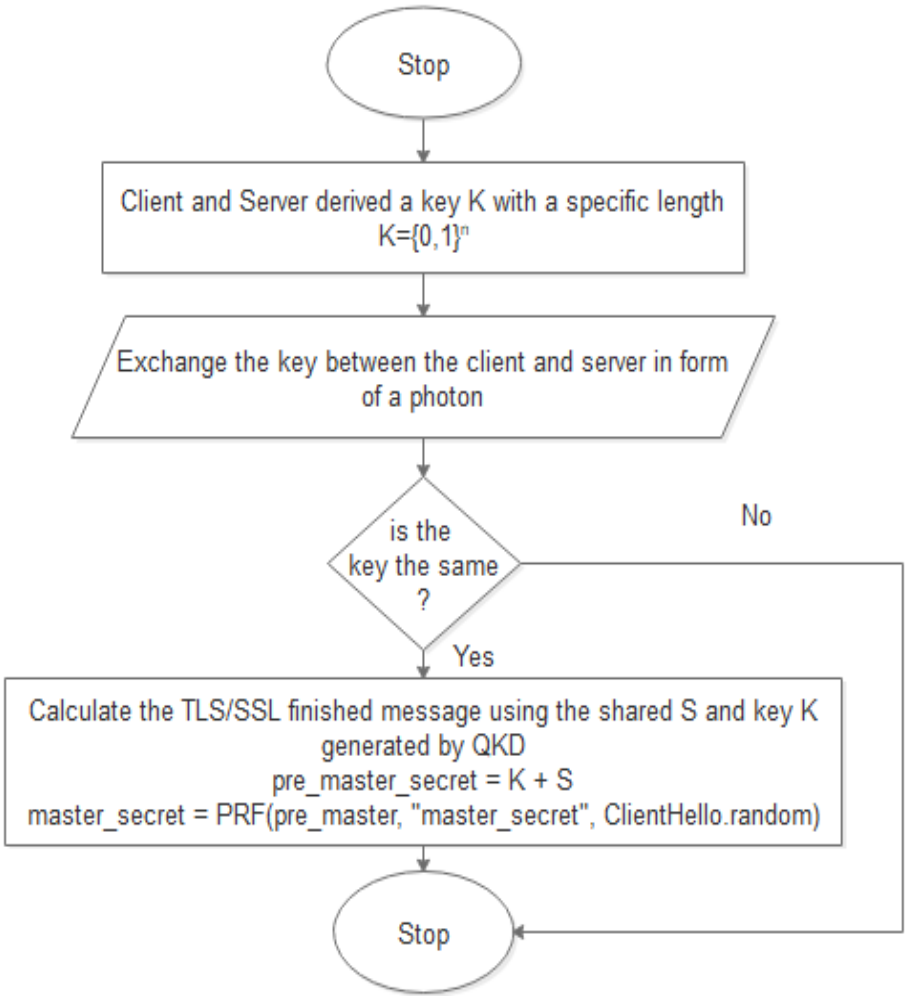

Figure 3.1: Flow Chart Diagram of the Research Methodology

3.3 Proposed Model

After a careful study in this research we proposed a model which can be used to integrate Quantum Key Distribution protocol into TLS/SSL cryptography protocol to detect the present of eavesdropper during TLS/SSL handshaking process which is vulnerable to Man-In-The-Middle (MITM) attack in internet-based environment.

i) **An optical channel**: QKD uses photons to encode information to exploit the laws of quantum physics. Now, there are two mediums to transport photons: the optical fiber or free space.

ii) **Optical modem:** the modem can play the role of detector and emitter of photons. The purpose of the optical modem is to detect and to send photons. All configuration is done on the modem.

iii) **Client/ users:** These are computer that make use of internet services.

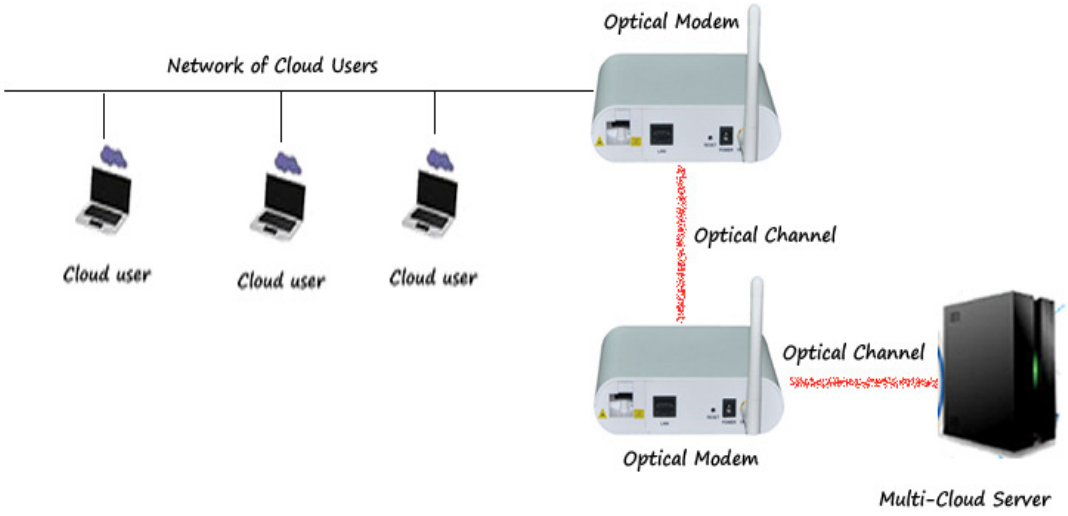

Figure 3.2: Proposed model to integrate QKD into TLS/SSL cryptography protocol handshaking process.

4. QKD SIMULATOR RESULT FOR THE MODEL

4.0.1 Simulator Result Using 600 Qubits With Eavedropping Enable

Initial Configuration							
Property Qubit Count	Basis choice bias delta	Eve basis choice bias delta	Eavesdropping	Eavesdropping rate	Error estimation sampling rate	Biased error estimation	Error tolerance
600	0.5	0.5	1	0.1	0.2	0	0.11

Figure 4.0: Initial parameters with 600 qubit

Statistics and Overview	
Property	**Value**
Initial number of qubits	600
Final key length	109
Estimated error	0.037
Eavesdropping enabled	1
Eavesdropping rate	0.1
Alice/Bob basis selection bias	0.5
Eve basis selection bias	0.5
Raw key mismatch before error correction	0.0332
Raw key mismatch after error correction	0
Information leakage (Total number of disclosed bits)	88
Overall key cost for authentication	256
Key length before error correction	217
Bit error probability	0.0323
Bits leaked during error correction	56
Shannon bound for leakage	45
Security parameter	20

Figure 4.2: Statistical overview result of the simulator

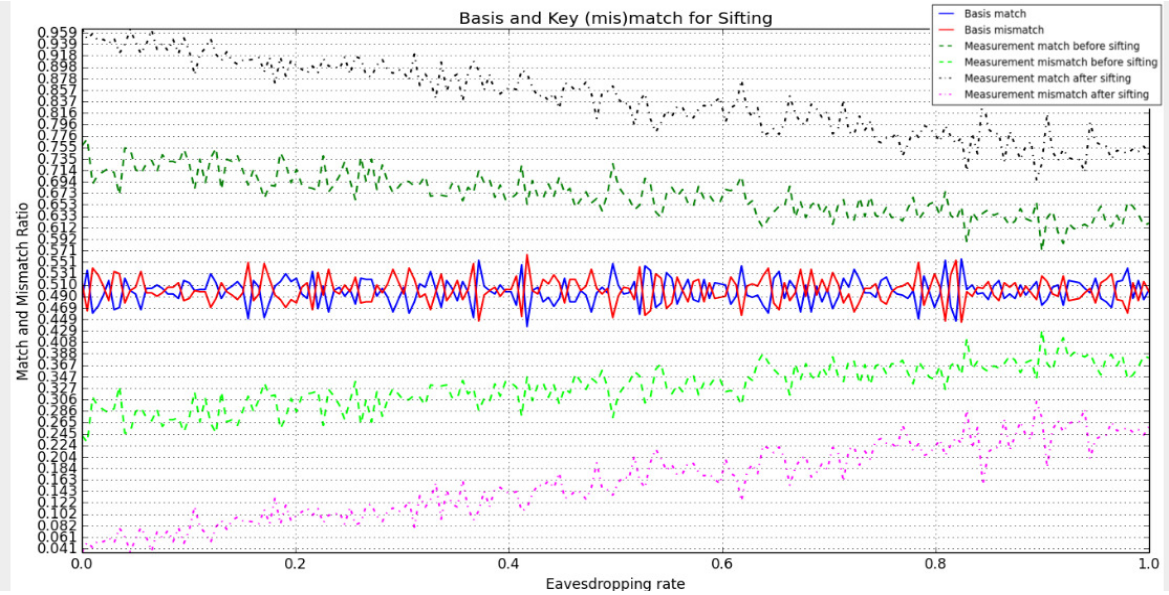

Figure 4.3: Eavesdropping rate against match and mismatch ratio

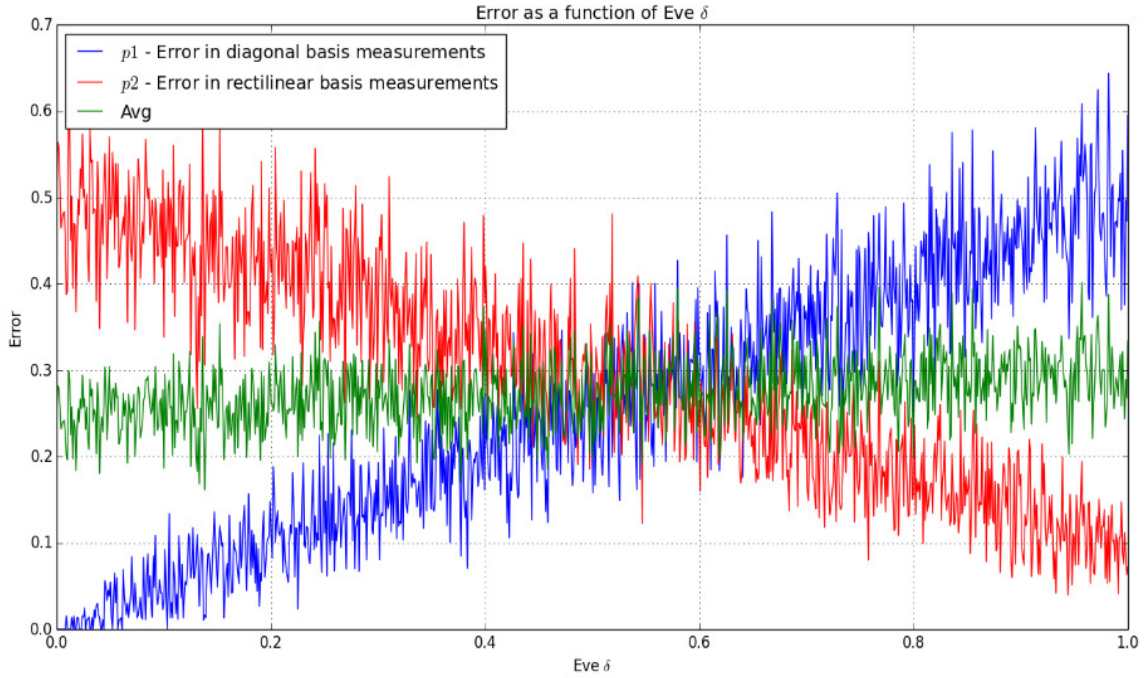

Figure 4.4: Measuring error as a function of eve.

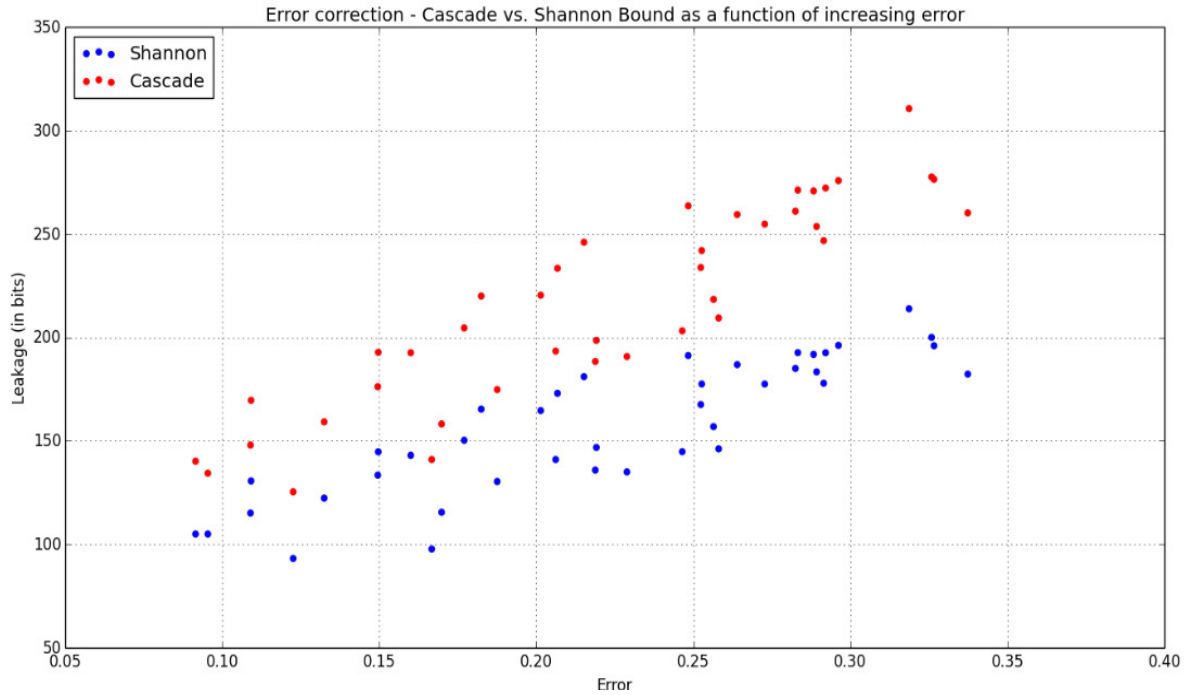

Figure 4.5: Measuring error against bit leakage

5. CONCLUSION

The result of this research, the test and evaluation of base on implementation and simulation demonstrated that the proposed system is more secured when compare with previous algorithms. Finally, the system have suggested an improved model which can be use in internet-based platform for internet users by enhancing the security aspect of internet environment using Quantum cryptography algorithm and SSL/TLS protocol. This model will be able to prevent internet environment from attack such as cipher suit rollback attack, eves dropping, insider attack and others. Furthermore, this research will help to increase end user trust.

REFERENCES

[1]. Alireza, R., Miika, K., Patrik, S., & Tuomas, .A. (2016). An SDN-Based Approach to Enhance the End-to-End Security: SSL/TLS Case Study, IEEE/IFIP Network Operations and Management Symposium (NOMS 2016).
[2]. Barhate, S. M., & Dhore, M. P. (2016). User Authentication Issues In Cloud Computing, 30–35.
[3]. Irvin, S. D. (2013). Data Security in Cloud Oriented Application Using SSL/TLS Protocol, International Journal of Application or Innovation in Engineering & Management (IJAIEM), Vol. 2, Issue. 12, pp. 80-85.
[4]. Olanrewaju, R. F., Islam, T., Khalifa, O. O., & Anwar, F. (2017). Cryptography as a Service (CaaS): Quantum Cryptography for Secure Cloud Computing, *10*(February). https://doi.org/10.17485/ijst/2017/v10i7/110897
[5]. Rajak, S., & Verma, A. (2012). Secure Data Storage in the Cloud using Digital Signature